Information security policy

The Society believes that despite the presence of threats to the security of such information, all security incidents are preventable.

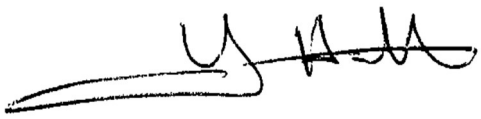
The Society is committed to

- Satisfying all applicable requirements related to information security
- Continual improvement of the information security management system
- achieving the objectives detailed in the policy through the following means:

1. The implementation and maintenance of an Information Security Management System (ISMS) that is independently certified as compliant with ISO 27001:2013
2. The systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures.
3. Regular monitoring of security threats and the testing/auditing of the effectiveness of control measures.
4. The maintenance of a risk treatment plan that is focussed on eliminating or reducing security threats.
5. The clear definition of responsibilities and authorities for implementing the ISMS.
6. The provision of appropriate information, instruction and training so that all employees are aware of their responsibilities and legal duties and can support the implementation of the ISMS.
7. The implementation and maintenance of the sub-policies documented within the system

The appropriateness and effectiveness of this policy and the means identified within it for delivering the Society's commitments will be regularly reviewed by Senior Management.

The implementation of this Information Security Policy and the supporting policies and procedures is fundamental to the success of the Society's business and must be supported by all employees as an integral part of their daily work and all suppliers who have an impact on.



Yvonne Hall Managing Director

23rd September 2020

Meg Heath Operations Director

23rd September 2020